WEST

Help | Logout | Interrupt

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers | Preferences

Search Results -

Terms	Documents
l9 and time	1

Database: US Patents Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Refine Search: `l9 and time` Clear

Search History

Today's Date: 11/7/2000

DB Name	Query	Hit Count	Set Name
USPT	l9 and time	1	L10
USPT	5414833.pn.	1	L9
USPT	l7 and detect$3 near3 pattern	1	L8
USPT	l6 and detect$3 near1 code	17	L7
USPT	l5 and network near1 security	495	L6
USPT	l1 or l2 or l3	20360	L5
USPT	l1 or l2 or l3	20360	L4
USPT	((380/$).ccls.)	5859	L3
USPT	((709/$).ccls.)	9374	L2
USPT	((713/$).ccls.)	7241	L1

WEST

Generate Collection

Search Results - Record(s) 1 through 1 of 1 returned.

☐ 1. Document ID: US 5414833 A

L10: Entry 1 of 1 File: USPT May 9, 1995

US-PAT-NO: 5414833
DOCUMENT-IDENTIFIER: US 5414833 A
TITLE: Network security system and method using a parallel finite state machine adaptive active monitor and responder

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWMC | Draw Desc | Image

Generate Collection

Terms	Documents
l9 and time	1

Display 10 Documents, starting with Document: 1

Display Format: TI Change Format

WEST

End of Result Set

Generate Collection

L10: Entry 1 of 1 File: USPT May 9, 1995

DOCUMENT-IDENTIFIER: US 5414833 A
TITLE: Network security system and method using a parallel finite state machine adaptive active monitor and responder

ABPL:
A system and method provide a security agent, consisting of a monitor and a responder, that respond to a detected security event in a data communications network, by producing and transmitting a security alert message to a network security manager. The alert is a security administration action which includes setting a flag in an existing transmitted protocol frame to indicate a security event has occurred. The security agent detects the transmission of infected programs and data across a high-speed communications network. The security agent includes an adaptive, active monitor using finite state machines, that can be dynamically reprogrammed in the event it becomes necessary to dynamically reconfigure it to provide real time detection of the presence of a suspected offending virus.

BSPR:
Today's high-speed (gigabit per second) multimedia networks consisting of WANs (wide area networks) and LANs (local area networks) can be thought of as a single computing resource comprised of many smaller computing resources spread over a large geographical area. The network as a whole provides network-wide services to its users, in a transparent fashion. It must be capable of communicating voice, image, and text, to name a few. In this new environment, the ability to monitor data flowing over a network, and the ability to react to anomalous conditions, in real time through appropriate network-level actions, seems fundamental to the maintenance of reliable network-wide services.

BSPR:
With pattern detection via a scanner, system files are periodically scanned for patterns, which consist of a set of pre-defined virus "signatures." Pattern matches are reported to the system manager who then decides whether the match represents a misdiagnosis or an actual viral infection. A virus consists of one or more fixed-length signature patterns, so the number of virus signatures is proportional to the number of viruses. A list of virus signatures must be maintained for each virus. The pattern search usually proceeds in a serial fashion, scanning each file one at a time, comparing the records of the file with each signature pattern in turn. This form of pattern

detection is not suitable for a high speed communications environment because of the delay caused by the serial, fixed-signature search pattern. In a high speed communications environment, it would be desirable to search for many different signature patterns in parallel.

BSPR:
Most security applications (including virus detection, natural language detection, and intrusion detection) consist of a detection step and a response step. The Hershey FSM information monitoring means described in U.S. pending patent application Ser. No. 08/138,045, cited above, is particularly suited as a pattern detection means in a high-speed communication environment. Yet for the Hershey FSM information monitoring means to be well-suited as a security device in a high-speed communication environment, it must be adapted to search for patterns particular to security applications and it must be extended to provide a capability for responding, in appropriate ways, to detected patterns. Such a security device (hereinafter called a security agent) must provide both an information monitoring function as well as a real-time responding function.

BSPR:
It is another object of the invention to provide a security agent with an information monitoring means that can be re-programmed in case it is necessary to dynamically reconfigure it to provide a capability in real-time to detect the presence of a suspected offending virus.

BSPR:
The security agent detects the transmission of infected programs and data across a high-speed communications network. The security agent includes an information monitoring means, consisting of adaptive, active monitor using finite state machines, that can be dynamically re-programmed in case it is necessary to dynamically reconfigure it to provide a capability in real-time to detect the presence of a suspected offending virus.

DRPR:
FIG. 10 is a block diagram illustration of another alternate embodiment of the invention wherein the Hershey adaptive, active monitor 100 of FIG. 4 is configured as an intrusion detector and responder 300 is designed to produce and transmit a security alert message whenever the number of detected pattern alarms of a particular type in a given interval of time reaches a prescribed threshold value.

DEPR:
In this manner, the speed of detection of a characteristic data pattern is increased, the number of components is decreased, and effective, real time control can be achieved for high speed data networks.

DEPR:
Further, the information collection means is coupled to the

network, and in response to receiving the event vector, outputs a control signal to the network to alter communication characteristics thereof. The resulting information collection architecture system provides a flexible, rapidly reconfigurable means to monitor and control data communications networks, through real time monitoring of the data patterns in their traffic.

DEPR:
In protocols having two characteristic data patterns with some of the component bit patterns being the same, the objective of pattern detection will be to detect either one of the two characteristic data patterns. In accordance with the adaptive active monitoring invention, the predecessor finite state machine will have a plurality of successor finite state machines which run simultaneously and parallel. The predecessor finite state machine will send a starting signal to both of the successor finite state machines, when the predecessor finite state machine has successfully detected the first component data pattern. The starting signal initializes both of the successor finite state machines to take over the analysis of the bit stream which follows the first component pattern, in order to look for the second component bit pattern or alternately the third component bit pattern. Both successor finite state machines run simultaneously and parallel and are mutually independent. They both run until one of them fails or one of them succeeds in finding its designated component bit pattern. In this manner, the speed of detection of a characteristic data pattern is increased, the number of components of the finite state machine array is decreased, and the effective real time control can be achieved for high speed data networks.

DEPR:
A security agent identifier 321 is included in security alert message 341 so that the messages' receiver will have proof of the identity of the security agent who has detected a pattern alarm and originated the security alert message. A sequence number counter 325 is included in security alert message 341 so that an adversary, who may intercept and replay security alert message 341 in bit stream 124, will be unable to cause the designated receiver to accept the security alert message as genuine. In an alternate embodiment of the invention, a time stamp can be used in place of sequence number counter 325 to prevent message replay attacks.

DEPR:
FIG. 8 is a block diagram illustration of an alternate embodiment of the invention (as described in FIG. 6) wherein the pattern alarms 144a, 144b, ..., 144n from the Hershey adaptive, active monitor 100 are applied to counters 360a, 360b, ..., 360n, respectively, in order to prevent adaptive, active monitor 100 of FIG. 4 from over-running responder 300. The sizes of counters 360a, 360b, ..., 360n are set so that the number of pattern alarm signals does not cause a counter overflow during the interval of time in which a security alert message is produced and transmitted. For example, 32-bit

counters are more than adequate to prevent counters from overflowing.

DEPR:
Referring now to FIG. 8, each pattern alarm signal 144i causes its associated counter 144i to be incremented by value +1, so that each counter records the numbers of respective pattern alarm signals produced by adaptive, active monitor 100. Processor 305 contains three processing functions, as follows: (1) counter scanning means 333, (2) security alert message production means 331, and (3) message authentication code production means 332. Counter scanning means 333 continually scans the counters, 360a, 360b, etc., searching for a non-zero counter value. When the final counter 360n is reached, the scanning continues with counter 360a, and so forth. When a non-zero counter value is detected, the counter value is read out and a security alert message and message authentication code are produced and transmitted. It is assumed that the process of reading out a counter value causes the counter to be reset to zero. In this way, the counter can continue to be updated during the time interval when a security alert message and message authentication code are produced and transmitted. Afterwards, counter scanning means 333 continues searching for a non-zero counter value--starting with the next counter in sequence following the counter that was just processed. Counter scanning means 333 also makes use of an index value representing the index of the counter currently being scanned. Upon detecting a non-zero counter value (via counter scanning means 333), processor 305 performs the following steps:

DEPR:
FIG. 9 depicts an extended security alert message 341 consisting of a security agent identifier 321, a security code 322, a sequence number counter 325, and a pattern alarm counter value 326. The extended security alert message 341 of FIG. 9 differs from the security alert message 341 of FIG. 7 in that the extended security alert message 341 of FIG. 9 contains a pattern alarm counter value 326. Pattern alarm counter value 326 represents the number of pattern alarms (with security code 322) detected by security agent 10 of FIG. 4 (with security agent identifier 321). Extended security alert message 341 can also contain a time-stamp instead of a sequence number counter. This would have the added advantage that a network security manager who receives the security alert message can easily calculate a rate (number of occurrences per standard interval of time) at which the security events are occurring.

DEPR:
FIG. 10 is a block diagram illustration of another alternate embodiment of the invention wherein the Hershey adaptive, active monitor 100 of FIG. 4 is configured as an intrusion detector and responder 300 is designed to produce and transmit a security alert message whenever the number of detected pattern alarms of a particular type in a given interval of time reaches a prescribed threshold value. Referring to FIG. 10, the Hershey adaptive, active monitor 100 of FIG. 4 is configured to scan bit stream 124 for three characteristic patterns,

specified in double quotation marks:

DEPR:
Responder 300 also contains a clock 350 which is attached to Hershey adaptive, active monitor 100 via line 372. Clock 350 is an incrementing counter. For each bit sampled in bit stream 124, a signal is sent via line 372 to clock 350, which causes the clock to increment by +1. When clock 350 reaches a predefined threshold value (e.g., the counter has a high-order one bit), program latch 302 is set. A clock size and threshold value are selected so that the time it takes to produce and transmit a security alert message is less than the time it takes clock 350 to cycle from zero to its threshold value. When processor 305 is not busy producing and transmitting a security alert message, processor 305 is busy monitoring program latch 302. When processor 305 detects that program latch 302 has been set, it reads the counter values (360a, 360b, and 360c), resets the counters to zero, and resets program latch 302. The counters are read and reset before the Hershey adaptive, active monitor is able to send another pattern alarm 144, thus preventing loss of information. Once the counters (360a, 360b, and 360c) have been read and reset, Hershey adaptive, active monitor continues, as before, sending pattern alarms (144a, 144b, and 144c). Processor 305 performs the following steps:

DEPR:
The Hershey, adaptive active monitor 100 is configured to scan for each of the 256 possible 8-bit characters in the data portion of each transmitted frame. The Hershey adaptive active monitor 100 accomplishes this scanning for the starting and ending delimiters for each the data block and then scanning and recording each character within each data block. A method for accomplishing this is taught by Hershey and Waclawsky in copending U.S. patent application entitled "System and Method for Adaptive, Active Monitoring of a Serial Data Stream Having a Characteristic Pattern," Ser. No. 08/138,045 cited above under Related Patents and Patent Applications. Responder 300 is designed to produce and transmit a security alert message whenever the distribution of detected characters in a given interval of time "looks" more like plaintext than ciphertext, which is based on a statistical calculation.

DEPR:
Referring to FIG. 11, the Hershey, adaptive, active monitor 100 of FIG. 4 is configured to scan bit stream 124 for any of the 256 characters within the data portion of a transmitted frame. Pattern alarm 144a corresponds to the 1st character, designated B`00000000`; pattern alarm 144b corresponds to the 2nd character, designated B`00000001`, ..., pattern alarm 144n corresponds to the 256th character, designated B`11111111`. For a given interval of time, counter 360a records the number of detected characters of the form B`00000000`, counter 360b records the number of detected characters of the form B`00000001`, ..., counter 360n records the number of detected characters of the form B`11111111`.

DEPR:

FIG. 12 is an example embodiment of pattern alarms and counters of FIG. 8 configured for virus detection. Referring to FIG. 12, the pattern alarms 144a, 144b, ..., 144n originating with adaptive, active monitor 100 of FIG. 4 are each uniquely associated with a particular characteristic viral pattern. Adaptive, active monitor 100 scans bit stream 124 for these virus patterns, which are character strings or patterns that uniquely identify each virus. As in FIG. 8, the pattern alarms 144a, 144b, ..., 144n from the Hershey adaptive, active monitor 100 are applied to counters 360a, 360b, ..., 360n, respectively. In this way, a clever adversary can not flood the network with viral agents hoping that some will escape detection by over running responder 300. The sizes of counters 360a, 360b, 360n are set so that the number of pattern alarm signals does not cause a counter overflow during the interval of time in which a security alert message is produced and transmitted. For example, 32-bit counters are more than adequate to prevent counters from overflowing. Otherwise, the processing steps to handle a detected virus are the same as those already described in and for FIG. 8.

DEPR:
Those skilled in the art will recognize that the viral patterns described in FIG. 12 may be static patterns or dynamically configurable patterns, depending on how adaptive, active monitor 100 is designed. The Hershey adaptive, active monitor is capable of dynamic re-configuration, thus enabling the security agent 10 to be updated in real_time to detect the presence of a suspected offending virus. Following such a re-configuration, which will also cause the type field associated with security code 322 to be adjusted so that each pattern alarm is uniquely associated with a corresponding virus type, both the adaptive, active monitor 100 and responder 300 of security agent 10 of FIG. 4 will operate normally as before.

DEPR:
A different application communications protocol can be implemented that allows a first application to transmit a new, unsolicited message to a second application. The first application need not wait for an acknowledgment, or a poll message, before transmitting a message to an intended recipient application. Furthermore, the first application can build a new message rather than intercepting and modifying an existing message on the network. The application addresses the message to a second application based on a hard-coded, non-volatile network address. Alternately, the address may be configured at application initialization or installation-time and stored in a volatile or nonvolatile storage.

DEPR:
Yet another application communications protocol can be implemented that allows a first application to multi-cast a message to two or more recipient applications. Again, the distribution list of network addresses is hard-coded in non-volatile storage or it may be configured at application initialization or installation-time and stored in volatile

storage. An application multi-casts a single message by transmitting the same message to two or more recipient applications, modifying only the destination address fields of the message.

DEPR:
FIG. 19 is a block diagram of the LLC sub-layer implementation within the Network Access Method 513 showing the construction of an L-PDU 570 from the input security alert message SAM 341 and the contents of the registers SSAP-REG 561 and DSAP-REG 562 of the Network Access Method 513. SSAP-REG 561 contains the source service access point address. DSAP-REG 562 contains the destination service access point address. Both the SSAP-REG and DSAP-REG register contents are loaded at system configuration time or are hard-coded. The SAM 513 is also input to the Control Field Production Means 563; the output of the Control Field Production Means 563 is put into the CONT field 573 of the L-PDU 570.